

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1. (previously presented) A method by which a mobile
2 subscriber with a WAP-enabled terminal can access a WEB or WAP
3 server, comprising the steps of:
4 said terminal sending a request for said server to a WAP
5 gateway, wherein encryption in the wireless interface
6 between said WAP-enabled terminal and said gateway is
7 based on WTLS (Wireless Transport Layer Security), and
8 wherein an encryption protocol used by said server is
9 based on one or both of the SSL or the TLS security
10 protocol; and
11 converting between WTLS and said one or both of the SSL or
12 the TLS security protocol in a secured domain of said
13 server administrated by an administrator,
14 wherein a plurality of WTLS encrypted packets sent by said
15 terminal are routed by said gateway to said secured
16 domain with said gateway not decrypting any portion of
17 at least some number of the encrypted packets
18 transported during a session.

1 2. (previously presented) Method according to claim 1,
2 wherein said gateway routes said packets to a proxy in said
3 secured domain, said proxy using at least one protocol layer of
4 the WAP protocol.

1 3. (previously presented) Method according to claim 2,
2 wherein said packets are routed according to one or both of the
3 URL or the domain name of the requested page in said gateway.

1 4. (previously presented) Method according to claim 2,
2 wherein said packets are routed by said gateway according to a
3 port number embedded in said packets.

1 5. (previously presented) Method according to claim 4,
2 wherein said encrypted packets are routed according to different
3 port numbers to different secured domains.

1 6. (previously presented) Method according to claim 4,
2 wherein said port number is extracted in an application layer of
3 said gateway from the URL of the requested page.

1 7. (original) Method according to claim 6, wherein said
2 port number is extracted from only a restricted number of
3 packets during a session, and wherein the routing of at least
4 one of the following packets depends on this extracted port
5 number.

1 8. (previously presented) Method according to claim 7,
2 wherein a proxy server in said secured domain extracts one or
3 both of the URL or the port number of the received packets and
4 wherein the proxy server sends back a command to said gateway if
5 it receives a packet with a different one or both of an URL or a
6 port number.

1 9. (previously presented) Method according to claim 4,
2 wherein said port number is extracted from said URL of the
3 required web page in said terminal.

1 10. (previously presented) Method according to claim 9,
2 wherein said port number is extracted by a browser from said URL
3 of the required web page.

1 11. (original) Method according to claim 8, wherein the
2 browser in said terminal only copies said port number in said
3 packets if an end-to-end secured connection is requested.

1 12. (original) Method according to claim 3, wherein said
2 packets in said gateway are routed to a secured domain if said
3 port number is comprised in a predefined range.

1 13. (previously presented) Method according to claim 3,
2 wherein said gateway sends a redirect command to said terminal
3 if an end-to-end secured connection is requested.

1 14. (previously presented) Method according to claim 13,
2 wherein said redirect command is time-limited.

1 15. (previously presented) Method according to claim 13,
2 wherein a proxy server in said secured domain extracts one or
3 both of the URL or the port number of the received packets and
4 sends a redirect command back to said terminal as soon as the
5 session is to be routed to said gateway.

1 16. (original) Method according to claim 13, wherein said
2 redirect command contains a forwarding address which is
3 extracted from a document made accessible by said WEB or WAP
4 server.

1 17. (original) Method according to claim 13, wherein said
2 redirect command contains a document which includes the
3 forwarding address.

1 18. (previously presented) A method according to claim 1,
2 by which a mobile user with a WAP-enabled terminal can access a
3 WEB or WAP server, wherein
4 said terminal sends a request for said server to said WAP
5 gateway, wherein a browser in said terminal extracts
6 the port number of the demanded WEB or WAP page and
7 copies it to packets sent to said gateway; and wherein
8 said packets are routed, using said gateway, according to
9 this port number.

1 19. (previously presented) A gateway comprising:
2 means for receiving packets WTLS-encrypted according to the
3 WTLS protocol from WAP-enabled terminals;
4 means for converting said packets into SSL-encrypted
5 requests; and
6 means for transmitting said SSL-encrypted requests to a
7 receiving server, wherein said gateway can recognize
8 WTLS-encrypted packets that are to be sent on
9 transparently and can convert said WTLS-encrypted
10 packets into said SSL-encrypted request without

11 decrypting the information contained in at least some
12 number of said WTLS-encrypted packets.

1 20. (previously presented) Gateway according to claim 19,
2 wherein said WTLS-encrypted packets are routed according to one
3 or both of the URL or the domain name of the requested page.

1 21. (previously presented) Gateway according to the claim
2 19, wherein said WTLS-encrypted packets are routed according to
3 the port number of the requested page.

1 22. (previously presented) Gateway according to claim 21,
2 wherein said WTLS-encrypted packets are routed to different
3 secured domains according to different port numbers.

1 23. (previously presented) Gateway according to claim 21,
2 wherein said port number is extracted from the URL of the
3 requested page in an application layer of said gateway.

1 24. (previously presented) Gateway according to claim 21,
2 wherein
3 said port number is extracted during a session only from a
4 restricted number of WTLS-encrypted packets, and
5 wherein
6 the routing of at least one following WTLS-encrypted packet
7 depends on said extracted port number.

1 Claim 25 (canceled).

1 26. (previously presented) A method for performing end-to-
2 end secure data transfer between a terminal and a server,

3 wherein said terminal is connected to said server via a wireless
4 connection between said terminal and a gateway, said method
5 comprising the steps of:

6 said terminal requesting a secure communication session
7 with said server via said gateway, said requesting
8 including the steps of:
9 said terminal generating a request including request
10 packets encrypted using a WTLS protocol,
11 said terminal sending said request to said gateway,
12 said gateway forwarding said request to said server or
13 to another server, wherein said gateway does not
14 decrypt all of said request packets, and
15 said server or said another server decrypting some
16 number of said request packets using said WTLS
17 protocol;

18 and

19 said server or said another server serving data to said
20 terminal via said gateway, said serving including the
21 steps of:

22 said server or said another server sending said data
23 including data packets encrypted using said WTLS
24 protocol to said gateway;

25 said gateway forwarding said data packets to said
26 terminal, wherein said gateway does not decrypt
27 any portion of at least some number of said data
28 packets; and

29 said terminal decrypting said data packets using said
30 WTLS protocol.

1 27. (previously presented) The method of claim 26, wherein
2 said gateway must decrypt some but not all of said request
3 packets to forward said request to said server or said another
4 server.

1 28. (previously presented) The method of claim 27, wherein
2 said gateway must decrypt some but not all of said data packets
3 to forward said data to said terminal.

1 29. (previously presented) The method of claim 26, wherein
2 a browser on said terminal provides information to said gateway
3 for forwarding said request to said server or said another
4 server without said gateway decrypting any of said request
5 packets.

1 30. (previously presented) The method of claim 29, wherein
2 said information includes one or more of: a port number, a
3 domain name, and an URL.

1 31. (previously presented) A system for performing end-to-
2 end secure data transfer between a terminal and a server, said
3 system comprising:

4 a gateway adapted for receiving a request for a secure
5 session with said server from the terminal, wherein
6 said request includes request packets encrypted using
7 a WTLS protocol, and wherein said gateway is also
8 adapted for forwarding said request to said server or
9 to another server, wherein said gateway does not

10 decrypt all of said request packets for performing
11 said forwarding;
12 said server or said another server adapted for decrypting
13 some number of said request packets using said WTLS
14 protocol and also adapted for serving data including
15 data packets encrypted using said WTLS protocol to
16 said gateway, wherein
17 said gateway forwards said data to said terminal without
18 decrypting any portion of at least some number of said
19 data packets, and wherein
20 the terminal decrypts said data packets using said WTLS
21 protocol.

1 32. (previously presented) The system of claim 31, wherein
2 said gateway must decrypt some but not all of said request
3 packets to forward said request to said server or said another
4 server.

1 33. (previously presented) The system of claim 32, wherein
2 said gateway must decrypt some but not all of said data packets
3 to forward said data to the terminal.

1 34. (previously presented) The system of claim 32, wherein
2 a browser on the terminal provides information to said gateway
3 for forwarding said request to said server or said another
4 server without said gateway decrypting any of said request
5 packets.

1 35 (previously presented) The system of claim 34, wherein
2 said information includes one or more of a port number, a domain
3 name, and an URL.

1 36. (previously presented) The method of claim 1, wherein
2 said gateway determines whether an end-to-end secured routing is
3 requested according to the URL of the requested page.

1 37 (previously presented) The gateway of claim 19, wherein
2 said gateway determines whether an end-to-end secured routing is
3 requested according to the URL of the requested page.